UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/675,159	09/29/2003	Richard Braun	67519.001038	5546

21967 7590 10/01/2007

HUNTON & WILLIAMS LLP
INTELLECTUAL PROPERTY DEPARTMENT
1900 K STREET, N.W.
SUITE 1200
WASHINGTON, DC 20006-1109

EXAMINER	
HIGA, BRENDAN Y	

ART UNIT	PAPER NUMBER
2153	

MAIL DATE	DELIVERY MODE
10/01/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No. 10/675,159	Applicant(s) BRAUN ET AL.	
	Examiner Brendan Y. Higa	Art Unit 2153	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *18 July 2007*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-27* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-27* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

Continued Examination Under 37 CFR 1.114

A request for continued examination under 37 CFR 1.114, including the fee set forth in 37 CFR 1.17(e), was filed in this application after final rejection. Since this application is eligible for continued examination under 37 CFR 1.114, and the fee set forth in 37 CFR 1.17(e) has been timely paid, the finality of the previous Office action has been withdrawn pursuant to 37 CFR 1.114. Applicant's submission filed on July 18, 2007 has been entered.

Claims 1-27 are pending.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Claims 1-7, 9-12, 13-19, and 21-27 are rejected under 35 U.S.C. 103(a) as being unpatentable over Chapman et al. (US 5774650) hereafter referred to as Chapman, in view of Dorfman et al. (US 6449651), hereafter referred to as Dorfman.

As per claim 1 and 25 Chapman discloses a method for using a utility (see access control program – Chapman column 6 lines 13-19; the program allows a permitted user

to make administrative configuration changes) at an end user device (see systems 2,4,6,8 - Chapman column 3 lines 20-22; the utility resides in the systems), comprising: assigning an elevated access right (see privilege user – Chapman column 4 lines 1-4, and establishing credentials upon login, see col. 5, lines 30-42) to a remote user identifier (see remote – Chapman column 3 lines 39-43, and user identity ["username"], see col. 5, lines 30-42, also see user number zero – Chapman column 4 lines 39-40; user with the identifier zero refers to having an elevated access) and a limited access right to an end user identifier (see normal user – Chapman column 4 lines 1-4 and col. 5, lines 30-42), the limited access right operable to prevent access to the utility at the end user device (see col. 6, lines 24-29); Accessing the utility at the end user device using the remote user identifier (access control program, see column 6 lines 20-24), the utility operable to allow the remote user identifier (see provide for privilege user – Chapman column 4 lines 4-6); to select an administrative tool at the end user device (see command line – Chapman column 6 lines 13-19; command line is the administrative tool used by a user with proper access rights to change or configure the end user system, also see "command line arguments" col. 6, lines 29-40) Launching the administrative tool according to the elevated access right while maintaining the limited access right of the end user identifier (see col. 6, lines 7-55, wherein the user having "super user" privileges accesses the control program, and issues a command warning other users [currently accessing the Unix system 2] (read as "normal users") of an impending access restriction. Thus, for at least a temporary "grace" period, the "super user", having access to the control program, and the "normal users" both have access

to the Unix system 2, according to their respective access privileges); and performing at least one administrative task at the end user device using the administrative tool (see col. 6, lines 54-col. 7, lines 31).

Chapman does not expressly teach temporarily assigning an elevated access right to the remote user identifier.

However, in the same art of computer remote accessing, Dorfman teaches a system and method for providing temporary access to a host computer from a remote computer (see abstract). The system includes the assignment of a "perishable" password that allows a network administrator, to connect to the host computer, to performing required maintenance, during predetermined temporary time periods (see col. 6, lines 27-43).

One of skill in the art would have been motivated to modify the teachings of Chapman with the teachings of Dorfman, in order to provide a secure temporary access by a network administrator (i.e. "superuser" described by Chapman) to a computer system from a remote location (see Dorfman, col. 2, lines 22-37).

As per claims 2 and 14 Chapman discloses, wherein assigning an elevated access right (see privilege user – Chapman column 4 lines 1-4) to a remote user identifier and a limited access right to an end user identifier further comprises: setting up at a network directory a remote user profile for the remote user identifier, the remote user profile associating the remote user identifier with the elevated access right (see Figure 2 and user account file – Chapman column 4 lines 23-26; also see super user denoted by user number zero – Chapman column 4 line 39-40); and setting up at the network directory

an end user profile, the end user profile associating the end user identifier with the limited access right (see Figure 2 and user account file – Chapman column 4 lines 23-26; also see create definition -Chapman line 56-57; the definition corresponds to the user name in the user account profile, and based on this the user has limited access right since the definition states the unauthorized users).

As per claim 3 and 15 Chapman discloses, wherein accessing the utility at the end user device using the remote user identifier further comprises receiving the remote user identifier (see login – Chapman column 5 lines 22-28; the username that is typed in is the remote user identifier); authenticating the remote user identifier using a network directory, the network directory comprising a profile associating the remote user identifier with the elevated access right (see authenticating and access rights – see Chapman column 5 lines 30-41; note that the account details is obtained from the user account file shown in figure 2); and granting access to the utility using the elevated access right (see invoke access control program and check that user is privilege to do so – Chapman column 6 lines 20-25).

As per claims 4,10,16 and 22 Chapman discloses, establishing a remote connection using a remote control module at a remote user device (see session can be opened with the remote system 2 using protocol – Chapman column 5 lines 18-22).

As per claims 5,11, 17 and 23 Chapman discloses, detecting a break in the remote Connection (see logging off – see Chapman column 7 lines 14-17; logging off breaks remote connection); and closing at least one process (see terminating all processes – Chapman column 7 lines 16-17), the at least one process corresponding to the administrative tool used to perform the administrative task (see exit access control program – Chapman column 7 lines 28-30).

As per claims 6,12,18 and 24 as best understood, Chapman discloses, wherein the remote user identifier is associated with the remote user device (see superuser – Chapman column 4 lines 39-40), the remote user device (see Chapman figure 1 block 12) located at a separate location (see other remote terminals – Chapman column 3 lines 39-43; note that the terminals are stated as remote therefore separate from the RISC System which corresponds to figure 1 block 2) from the end user device (see Chapman figure 1 block 2).

As per claims 7 and 19 Chapman discloses, wherein the administrative task comprises operations that affect the settings of the end user device (command line arguments supplied – Chapman column 6 lines 29-36; the command line arguments are the administrative tasks that will affect settings at the end user device, which includes restricting access).

As per claims 9, 21 and 26, Chapman discloses a method and software of elevating an access right at an end user device comprising: receiving an authentication message from a network in response to a login request from a remote user identifier (see authenticating and access rights – see Chapman column 5 lines 30-41; note that the account details is obtained from the user account file shown in figure 2), the authentication message operable to inform if the remote user identifier is associated with an elevated access right, the elevated access right operable to allow access to an administrative tool at the end user device (see invoke access control program and check that user is privilege to do so – Chapman column 6 lines 20-25); generating an elevated access layer using the elevated access right, the elevated access layer operable to: initiate an administrative tool at the end user device (see invoke access control program and check that user is privilege to do so – Chapman column 6 lines 20-25); and elevate the access right of the remote user identifier according to the elevated access right (see privilege user – Chapman column 4 lines 1-4); launching the administrative tool using the elevated access layer (see entering command – Chapman column 6 lines 20-22); and processing at least one administrative task at the end user device using the administrative tool while the end user identifier retains the limited access right to the end user device (see col. 6, lines 7-55, wherein the user having "super user" privileges accesses the control program, and issues a command warning other users [currently accessing the Unix system 2] (read as "normal users") of an impending access restriction. Thus, for at least a temporary "grace" period, the "super user", having access to the control program, and the "normal users" both have access

to the Unix system 2, according to their respective access privileges); the limited access right operable to prevent access to the administrative tool at the end user device (see col. 3, line 66-col. 4, line 9 and col. 6, lines 20-29, *"In Unix terms the privileged user must have superuser authority having a unique user identification number 33 of zero"*). Chapman does not expressly teach the elevated access right being a temporarily elevated access right to the remote user identifier.

However, in the same art of computer remote accessing, Dorfman teaches a system and method for providing temporary access to a host computer from a remote computer (see abstract). The system includes the assignment of a "perishable" password that allows a network administrator, to connect to the host computer, to performing required maintenance, during predetermined temporary time periods (see col. 6, lines 27-43). One of skill in the art would have been motivated to modify the teachings of Chapman with the teachings of Dorfman, in order to provide a secure temporary access by a network administrator (i.e. "superuser" described by Chapman) to a computer system from a remote location (see Dorfman, col. 2, lines 22-37).

As per claim 13, Chapman discloses, a system for elevating access rights of a remote user, comprising: a network directory operable to assign an elevated access right to a remote user identifier and a limited access right to an end user identifier (see Figure 2 and user account file – Chapman column 4 lines 23-26; also see super user denoted by user number zero – Chapman column 4 line 39-40); a utility stored (access control program – Chapman column 4 lines 2-4) at an end user device and operable to: launch

the administrative tool according to the elevated access right while the end user identifier retains the limited access rights to the end user ((see col. 6, lines 7-55, wherein the user having "super user" privileges accesses the control program, and issues a command warning other users [currently accessing the Unix system 2] (read as "normal users") of an impending access restriction. Thus, for at least a temporary "grace" period, the "super user", having access to the control program, and the "normal users" both have access to the Unix system 2, according to their respective access privileges), the limited access right operable to prevent access to the utility at an end user device (see col. 3, line 66-col. 4, line 9 and col. 6, lines 20-29, *"In Unix terms the privileged user must have superuser authority having a unique user identification number 33 of zero"*) and perform at least one administrative task at the end user device using the administrative tool (see col. 6, lines 54-col. 7, lines 31); and a remote (see remote – Chapman column 3 lines 39-43) user device (see Chapman figure 1 block 12) operable to access the utility at the end user (access control program – Chapman column 4 lines 2-4) device using the remote user identifier (see provide for privilege user – Chapman column 4 lines 4-6) in order to perform the at least one administrative task at the end user device (see col. 6, lines 54-col. 7, lines 31).

Chapman does not expressly teach the elevated access right being a temporarily elevated access right to the remote user identifier.

However, in the same art of computer remote accessing, Dorfman teaches a system and method for providing temporary access to a host computer from a remote computer (see abstract). The system includes the assignment of a "perishable" password that

allows a network administrator, to connect to the host computer, to performing required maintenance, during predetermined temporary time periods (see col. 6, lines 27-43). One of skill in the art would have been motivated to modify the teachings of Chapman with the teachings of Dorfman, in order to provide a secure temporary access by a network administrator (i.e. "superuser" described by Chapman) to a computer system from a remote location (see Dorfman, col. 2, lines 22-37).

As per claim 27, Chapman discloses, a method of elevating an access right at an end user device, comprising: receiving an authentication message from a network in response to a login request from a remote user identifier (see authenticating and access rights – see Chapman column 5 lines 30-41; note that the account details is obtained from the user account file shown in figure 2), the authentication message operable to inform if the remote user identifier is associated with an elevated access right, the elevated access right operable to allow access to an administrative tool at the end user device, (see invoke access control program and check that user is privilege to do so – Chapman column 6 lines 20-25). the remote user identifier associated with a remote user device (see superuser – Chapman column 4 lines 39-40), the remote user device (see Chapman figure 1 block 12) being at a separate location from the end user device (see Chapman figure 1 block 2); generating an elevated access layer using the elevated access right, the elevated access layer operable to: initiate an administrative tool at the end user device (see invoke access control program and check that user is privilege to do so – Chapman column 6 lines 20-25); and elevate the access right of the remote

user identifier according to the elevated access right (see privilege user – Chapman column 4 lines 1-4); launching the administrative tool using the elevated access layer, while the end user identifier retains the limited access rights to the end user device (see col. 6, lines 7-55, wherein the user having "super user" privileges accesses the control program, and issues a command warning other users [currently accessing the Unix system 2] (read as "normal users") of an impending access restriction. Thus, for at least a temporary "grace" period, the "super user", having access to the control program, and the "normal users" both have access to the Unix system 2, according to their respective access privileges); and processing at least one administrative task at the end user device using the administrative tool while maintaining an end user identifier logged into the network with a limited access right (see col. 6, lines 7-55, wherein the user having "super user" privileges accesses the control program, and issues a command warning (read as a administrative task) to other users [currently accessing the Unix system 2] (read as "normal users") of an impending access restriction. Thus, for at least a temporary "grace" period, the "super user", having access to the control program, and the "normal users" both have access to the Unix system 2, according to their respective access privileges), the limited access right operable to prevent access to the administrative tool at the end user device (see col. 3, line 66-col. 4, line 9 and col. 6, lines 20-29, *"In Unix terms the privileged user must have superuser authority having a unique user identification number 33 of zero"*); detecting a remote connection from the remote user device, the remote connection operable to access the end user device using a remote control module at the remote user device (see session can be opened

with the remote system 2 using protocol – Chapman column 5 lines 18-22); and discontinuing (see logging off – see Chapman column 7 lines 14-17; logging off breaks remote connection) at least one process (see terminating all processes – Chapman column 7 lines 16-17), associated with the administrative tool upon detecting a break in the remote connection (see exit access control program – Chapman column 7 lines 28-30).

Chapman does not expressly teach the elevated access right being a temporarily elevated access right to the remote user identifier.

However, in the same art of computer remote accessing, Dorfman teaches a system and method for providing temporary access to a host computer from a remote computer (see abstract). The system includes the assignment of a "perishable" password that allows a network administrator, to connect to the host computer, to performing required maintenance, during predetermined temporary time periods (see col. 6, lines 27-43).

One of skill in the art would have been motivated to modify the teachings of Chapman with the teachings of Dorfman, in order to provide a secure temporary access by a network administrator (i.e. "superuser" described by Chapman) to a computer system from a remote location (see Dorfman, col. 2, lines 22-37).

Claims 8 and 20 are rejected under 35 U.S.C. 103(a) as being unpatentable over Chapman (US 5774650), in view of Dorfman (US 6449651), in further view of Meyer et al (US 6289378), hereafter referred to as Meyer.

As per claim 8 and 20, Chapman discloses all the limitations of parent claims 1 and 13 from which claims 8 and 20 depend, respectively (see above 102 rejections for claim 1 and 13).

Chapman does not disclose expressly wherein the end user device comprises an operating system selected from a group consisting of WINDOWS XP and WINDOWS 2000.

The concept of using Windows as operating system is well known in the art as illustrated by Meyer which teaches an end user device comprises an operating system selected from a group consisting of WINDOWS XP and WINDOWS 2000 (see Windows column 4 lines 61-64).

Meyer and Chapman are analogous art because both have a similar problem solving area, which is to restrict access to users based on the definitions of authorized users. At the time of the invention, it would have been obvious to a person of ordinary skill in the art to modify the system of Chapman with a user device comprises an operating system selected from a group consisting of windows such as disclosed by Meyer et al. The motivation is to provide a platform independent system so as to incorporate comparable devices that are widely used, such as a device that runs on the Windows environment.

Response to Arguments

Applicant's arguments with respect to claims 1-27 have been considered but are moot in view of the new ground(s) of rejection.

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Brendan Y. Higa whose telephone number is (571)272-5823. The examiner can normally be reached on M-F 8:30-5:00.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Glenton Burgess can be reached on (571)272-3949. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

BYH

GLENTON B. BURGESS
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100